From the editors…

In this issue, David Smith and Tim Lee consider the practical implications of data breach notifications by Australian organisations in light of the current privacy regime which does not explicitly mandate such notifications, proposed mandatory data breach notification laws in Australia and the experience of other jurisdictions where such laws exist.

John D Fitzgerald introduces us to the use of graph theory – the mathematical study of the collection of things related in some way to one another – in legal interpretation, and provides a demonstration by applying it to the structure and definitions of the *Health Practitioner Regulation National Law 2009* (NSW).

Finally, Pamela and Xenogene Gray explore the potential for better governmental administration and decision-making via the use of computerised logic systems capable of mapping complex rule systems and automating their application to a specific case. Their article illustrates how the superexpert shell eGanges in particular could have been used as a quality control tool to improve outcomes under the former federal government's home insulation scheme.

The Editors
Daniel Thompson, Isaac Lin, David Ng and Moses Kakaire

The Office of the Australian Information Commissioner (OAIC)[1] adopts the following definition in its *Guide to Handling Personal Information Security Breaches*[2] (Data Breach Notification Guide):

> "Data breach means, for the purpose of this guide, when personal information held by an agency or organisation is lost or subject to unauthorised access, use, modification, disclosure, or other misuse."

This definition reflects the language of Australian Privacy Principle (APP) 11 (formerly National Privacy Principle 4 and Information Privacy Principle 4), which requires organisations to take "reasonable steps" to protect personal information they hold from:

- misuse, interference[3] and loss; and
- unauthorised access, modification or disclosure.

This raises two important points about the concept of a "data breach". The first is that a "data breach" is not necessarily a breach of the APPs – rather, the word "breach" refers to the breach of the organisation's information security. Whether this security breach is a breach of the APPs will depend on whether the organisation's information security measures were sufficient in light of APP 11. Given this distinction, many organisations now choose to use language that more specifically describes the nature of the incident and which avoids connotations of fault – for example, "security incident".

The second important point about the definition is that it is not limited to malicious actions, such as theft or "hacking" (although the term "data breach" is commonly used to refer to such actions). It also includes situations where an organisation's mishandling of personal information results in misuse or accidental loss or disclosure (e.g. sending correspondence to the wrong address).

The Data Breach Notification Guide provides the following examples of situations that could give rise to a data breach:

- lost or stolen laptops or paper records containing personal information;
- databases containing personal information being hacked into or otherwise illegally accessed by external parties;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins; and
- an organisation mistakenly providing personal information to the wrong person.

In addition to these examples, a number of the OAIC's recent data breach investigations have concerned situations where networked records were stored on a publically accessible web server that did not have appropriate security controls and became discoverable via search engines. Recent examples include Multicard Pty Ltd (May 2014)[4], Telstra Corporation Limited (March 2014)[5] and Medvet Science Pty Ltd (July 2012)[6].

Is notification mandatory?

There is no specific obligation in the Privacy Act that requires an organisation to notify affected individuals (or the OAIC) of a data breach.

However, the OAIC considers that a requirement to notify affected individuals may form part of an organisation's general data security obligations under what is now APP 11.1. The Data Breach Notification Guide summarises the OAIC's position in the following terms:

> "*(R)easonable steps [to protect personal information under what is now APP 11.1] may include the preparation and implementation of a data breach policy and response plan. Notification of the*